

Claims

1. A internal security method for a relational database system, comprising the steps of:

(a) determining which data information from the total amount of data information stored in system databases is restricted data information that shall not be accessible by each and every 1 to N system users, where N is an integer greater than 1;

(b) determining for each system user the restricted data information that such a system user shall have access;

(c) creating at least one relational access table with each system user having at least one record in the relational access table that is keyed to that system user's access to the restricted data information that was determined at step (b); and

(d) each system user accessing restricted data information stored in the system databases according to the relational access table created at step (c).

2. The method as recited in claim 1, wherein the relational database is a structured query language database.

3. The method as recited in claim 1, wherein each relational access table has a foreign key that relates to a primary key of only one system user.

4. The method as recited in claim 1, wherein each relational access table created at step (c) may have access to additional restricted data information added to it by updating the relational access table after it is created.

5. The method as recited in claim 1, wherein each relational access table created at step (c) may have access to certain restricted data information deleted from it by updating the relational access table after it is created.

6. The method as recite in claim 1, wherein the relational database system that incorporates the internal security method includes a star schema configuration.

7. The method as recite in claim 6, wherein the relational database system that incorporates the internal security method includes a full star schema configuration.

8. A internal security method for a relational database system, comprising the steps of:

(a) determining which data information from the total amount of data information stored in system databases is restricted data information that shall not be accessible by each and every 1 to N system users, where N is an integer greater than 1;

(b) determining for each system user the restricted data information that such a system user shall have access;

(c) determining the hierarchical level of access for each system user with regard to the restricted data information;

(d) determining for at least two system users, based on the hierarchical level of access determination at step (c), that a second system user with a lower hierarchical level of access has access to the restricted data information that is a subset of the restricted data information to which a first system user with a higher hierarchical level of access has access;

(e) creating at least one relational access table for controlling the first and second system users' access to restricted data information such that the first system user will have one or more records in the relational access table that is keyed to the first system user's access to restricted data information that is determined at step (b) joined with the second system user's access to restricted data information that is determined at step (b), and the second system user will have one or more records in the relational access table that is keyed to the second system user's access to restricted data information that is determined at step (b); and

(f) the first and second system users accessing restricted data information stored in the system databases according to the relational access table created at step (e).

9. The method as recited in claim 8, wherein the relational database is a structured query language database.

10. The method as recited in claim 8, wherein each relational access table has a foreign key that relates to a primary key of only one system user.

11. The method as recited in claim 8, wherein each relational access table created at steps (e) and (f) may have access to additional restricted data information added to them by updating the relational access table after they are created.

12. The method as recited in claim 8, wherein each relational access table created at steps (e) and (f) may have access to certain restricted data information deleted from them by

updating the relational access table after they are created.

13. The method as recite in claim 8, wherein the relational database system that incorporates the internal security method includes a star schema configuration.

14. The method as recite in claim 13, wherein the relational database system that incorporates the internal security method includes a full star schema configuration.

15. A internal security method for a relational database system, comprising the steps of:

(a) determining which data information from the total amount of data information stored in system databases is restricted data information that shall not be accessible by each and every 1 to N system users, where N is an integer greater than 1;

(b) determining for each system user the restricted data information that such a system user shall have access;

(c) determining the hierarchical level of access for each system user with regard to the restricted data information;

(d) determining for at least two system users, based on the hierarchical level of access determination at step (c), that a second system user with a lower hierarchical level of access has access to the restricted data information that includes other than a subset of the restricted data information to which a first system user with a higher hierarchical level of access has access;

(e) creating at least one relational access table for controlling the first and second system users' access to restricted data information such that the first system user will have one or more records in the relational access table that is keyed to the first system user's access to restricted data information that is determined at step (b) joined with the second system user's access to restricted data information that is determined at step (b), and the second system user will have one or more records in the relational access table that is keyed to the second system user's access to restricted data information that is determined at step (b); and

(f) the first and second system users accessing restricted data information stored in the system databases according to the relational access table created at steps (e).

16. The method as recited in claim 15, wherein the relational database is a structured query language database.

17. The method as recited in claim 15, wherein each relational access table has a foreign key that relates to a primary key of only one system user.

18. The method as recited in claim 15, wherein each relational access table created at steps (e) and (f) may have access to additional restricted data information added to them by updating the relational access table after they are created.

19. The method as recited in claim 15, wherein each relational access table created at steps (e) and (f) may have access to certain restricted data information deleted from them by updating the relational access table after they are created.

20. The method as recite in claim 15, wherein the relational database system that incorporates the internal security method includes a star schema configuration.

21. The method as recite in claim 20, wherein the relational database system that incorporates the internal security method includes a full star schema configuration.

22. A internal security method for a relational database system, comprising the steps of:

(a) determining which data information from the total amount of data information stored in system databases is restricted data information that shall not be accessible by each and every 1 to N system users, where N is an integer greater than 1;

(b) determining for each system user the restricted data information that such a system user shall have access;

(c) determining the hierarchical level of access for each system user with regard to the restricted data information;

(d) determining for at least two system users, based on the hierarchical level of access determination at step (c), that a second system user with a lower hierarchical level of access has access to the restricted data information that is a subset and includes other than a subset of the restricted data information to which a first system user with a higher hierarchical level of access has access;

(e) creating at least one relational access table for controlling the first and second system users' access to restricted data information such that the first system user will have one or more records in the relational access table that is keyed to the first system user's access to restricted

data information that is determined at step (b) joined with the second system user's access to restricted data information that is determined at step (b), and the second system user will have one or more records in the relational access table that is keyed to the second system user's access to restricted data information that is determined at step (b); and

(f) the first and second system users accessing restricted data information stored in the system databases according to the relational access table created at steps (e).

23. The method as recited in claim 22, wherein the relational database is a structured query language database.

24. The method as recited in claim 22, wherein each relational access table has a foreign key that relates to a primary key of only one system user.

25. The method as recited in claim 22, wherein each relational access table created at steps (e) and (f) may have access to additional restricted data information added to them by updating the relational access table after they are created.

26. The method as recited in claim 22, wherein each relational access table created at steps (e) and (f) may have access to certain restricted data information deleted from them by updating the relational access table after they are created.

27. The method as recite in claim 22, wherein the relational database system that incorporates the internal security method includes a star schema configuration.

28. The method as recite in claim 27, wherein the relational database system that incorporates the internal security method includes a full star schema configuration.